Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

journal homepage: www.elsevier.com/locate/engappai

Survey Paper

Fault detection, diagnosis and recovery using Artificial Immune Systems: A review

Nawel Bayar[a], Saber Darmoul[b], Sonia Hajri-Gabouj[a], Henri Pierreval[c]

[a] LISI, Institut National des Sciences Appliquées et de Technologie, B.P. 676, Centre Urbain Nord, 1080 Tunis, Tunisia
[b] Industrial Engineering Department, King Saud University, P.O. Box 800, Riyadh 11421, Saudi Arabia
[c] LIMOS, UMR – CNRS 6158, Clermont University, IFMA, CS 20265, F-63175 Aubière, France

ARTICLE INFO

Article history:
Received 10 February 2015
Received in revised form
12 June 2015
Accepted 7 August 2015
Available online 16 September 2015

Keywords:
Manufacturing systems
Fault
Detection
Diagnosis
Recovery
Artificial Immune Systems
Review

ABSTRACT

Biological immunity is a natural system that protects a host organism against disease causing elements threatening its normal functioning. It offers many interesting features that inspired the design of Artificial Immune Systems (AIS) to solve several kinds of engineering problems. As a manufacturing system can be assimilated to a host organism, while process anomalies (e.g. faults, errors and failures) can be considered as disease causing elements, biological immunity is particularly inspiring approaches for fault detection, diagnosis and recovery (FDDR). Although many interesting works and different adaptations were suggested, we are not aware of any recent survey that would aim at reviewing works, synthesizing modeling approaches and reporting on results in this field. This paper provides a recent survey and an analysis framework to fill in this gap. After a first part overviewing FDDR needs and requirements, we introduce biological immunity and highlight the main concepts and mechanisms that are particularly relevant to FDDR problems. The numerous works analyzed distinguish three categories of AIS: one-signal (for positive and negative selection) based approaches, two-signal (for danger and NK) based approaches and immune network based approaches. We suggest a possible architecture for FDDR systems, and organize the immune system concepts, components and mechanisms in such a way to show how they are applied for each of the detection, diagnosis and recovery tasks. Our analysis allows an overview of current technical and methodical developments in this field and foresight of future research perspectives.

1. Introduction

In manufacturing industries, processes, machines and related equipment are fundamental technical systems that provide the physical platform and technology needed to economically produce high-quality products in the required volumes. The operating conditions under which these technical systems work play a critical role in satisfying customer requirements and demands. With the increasing level of complexity of manufacturing processes and machines, there is an increased need for more effective and efficient techniques to monitor machine conditions in real time, detect the inception, progression and propagation of faults, errors and defects, and enable suitable decision making, before such anomalies result in damageable failures, interruptions and downtime. Such techniques are a prerequisite for realizing reliable, economical, environment-friendly, and ultimately, intelligent manufacturing and product quality control (Wang and Gao, 2006).

Process monitoring refers to the acquisition, manipulation and analysis of sensor measurements to determine the state of the process (Ulsoy, 2006). For this purpose, a process set of variables (e.g. force, speed, motion, temperature, pressure, power, acoustic emission, feed motor current, etc.) are measured, processed online and compared to their expected values. Any deviations from expected values are attributed to process anomalies (e.g. faults, errors, failures, malfunctions, etc.; cf. Section 2.1 for terminology). A process anomaly could be gradual, such as tool/wheel wear; may be abrupt, such as tool breakage; or may be preventable, such as excessive vibration/chatter. Knowledge of tool wear is necessary for scheduling tool changes; detection of tool breakage is important for saving the work piece and/or the machine; and identifying chatter is necessary for triggering corrective decisions (Ulsoy, 2006). Monitoring is necessary to prevent machine damage by stopping the process, or to remove the anomaly by adjusting the process inputs (e.g. feeds and speeds).

E-mail addresses: bayarnawel86@gmail.com (N. Bayar), sdarmoul@ksu.edu.sa (S. Darmoul), sonia.gabouj@insat.rnu.tn (S. Hajri-Gabouj), henri.pierreval@ifma.fr (H. Pierreval).

http://dx.doi.org/10.1016/j.engappai.2015.08.006
0952-1976/© 2015 Elsevier Ltd. All rights reserved.

Process monitoring is usually achieved based on interactions between human operators, hardware and software technologies. Operators routinely perform monitoring tasks; for example, visually detecting missing and broken tools and detecting chatter from the characteristic sound it generates. Monitoring algorithms rely on filtered/fused sensor measurements, which, along with operator inputs, determine the process state. As it will be discussed in more detail in Section 3, process monitoring is faced with some limitations due to technological constraints (e.g. number, location, robustness and reliability of sensors) and modeling restrictions (availability, complexity and accuracy of analytical models). Such limitations call for the design and development of sophisticated signal processing of sensor measurements, based on thresholding or artificial intelligence (AI) techniques to assist operators and decision makers in achieving the tasks of fault detection, diagnosis and recovery.

These last years, Artificial Immune Systems (AISs) have attracted an increasing number of researchers in the area of Artificial Intelligence. AIS are computational intelligence techniques inspired from biological immunity and directed towards engineering problem solving (De Castro and Timmis, 2002). AIS have been applied to a wide range of manufacturing problems, including scheduling (Darmoul et al., 2006), automation, monitoring, control (Darmoul et al., 2013), robotics (Raza and Fernandez, 2012), optimization(Gao and Wang, 2010), etc. AIS have been extensively investigated and applied in computer systems and networks, to improve security and detect anomalies, which in this field refer to intrusions and malware detection and prevention (Swimmer, 2007). Our investigation does not focus on anomaly detection in computer systems and networks, but on anomaly detection in technical systems in manufacturing industries (i.e. difference in application domain). As it will be discussed in more detail in Sections 2 and 3, manufacturing systems rely on technical components, and involve processes and machines, which operating conditions, features and requirements are different from computer systems and networks.

Many efforts focused on developing AIS for anomaly detection, diagnosis and recovery in technical systems (Dasgupta et al., 2011; Dasgupta, 2006). Such efforts are based on different interpretations of immune concepts, components and mechanisms that led to different implementations of AIS. Unfortunately, we are not aware of any recent survey that would aim at reviewing works, making the inventory of analogies, synthesizing modeling approaches to show the differences in points of view between them and to report on results relative to the performance of AIS-based fault detection, diagnosis and recovery (FDDR). This paper provides a recent survey that tries to fill in this gap by addressing some key issues, such as what are the needs and requirements for FDDR in technical systems that AIS allow tacking into account? What are the main features of AIS that can be adapted to FDDR problems? How are these features adapted to FDDR problems? What are the domains in which AIS have been applied successfully to solve FDDR problems? To address these issues, we analyze literature based on a classification of existing AIS approaches in order to highlight the main immune concepts and mechanisms relevant to FDDR problems and to explain how they were applied for each of the detection, diagnosis and recovery tasks. We hope our analysis contributes to have better understanding of current technical and methodical developments in this field and to foresee future research perspectives.

Therefore, the paper is organized as follows: Section 2 introduces fault detection, diagnosis and recovery (FDDR) problems. Section 3 overviews the main features and principles of the biological immune system and presents analogies with FDDR concerns. Section 4 describes our review methodology to realize this survey. Section 5 shows how AIS concepts and mechanisms have been adapted to tackle FDDR. Section 6 discusses current solutions and issues and suggests some further research directions. Finally, Section 7 concludes the paper and draws several opened research directions.

2. Fault detection, diagnosis and recovery

The monitoring of technical processes is aimed at showing the present state, indicating undesired, unacceptable or intolerable states, and taking appropriate actions to avoid damage or accidents (Isermann, 2006). Process anomalies originate from deviations from normal/acceptable/tolerable process behavior and can be attributed to many causes. They may result in malfunctions or failures if no recovery decisions are taken.

2.1. Terminology

To serve the purposes of the literature analysis that will be conducted in next sections, we recall the following definitions, which were introduced by the IFAC symposium and technical committee on fault detection, supervision and safety for technical processes (SAFEPROCESS), and published in Isermann and Ballé (1997) and Isermann (2006).

- **A fault** is an unpermitted deviation of at least one characteristic property (feature) of the system from the acceptable, usual, standard operating condition.
- **An error** is a deviation between a computed value (of an output variable) and the true, specified or theoretically correct value.
- **A failure** is a permanent interruption of a system's ability to perform a required function under specified operating conditions.
- **A malfunction** is an intermittent irregularity in the fulfilment of a system's desired function.
- **A disturbance** is an unknown (and uncontrolled) input acting on a system.
- **A perturbation** is an input acting on a system, which results in a temporary departure from steady state.
- **A residual** is a fault indicator, based on deviations between measurements and model equation based calculations.
- **A symptom** is a change of an observable quantity from normal behavior.

As an example, in a manufacturing system, a deviation from the required temperature of a machine is a machine fault. If the machine is unable to realize its function correctly, then it is a machine failure. If the machine stops and does not fulfill its role within a process plan anymore, then the function realized on this machine is interrupted, therefore leading to a system malfunction. This paper mainly focuses on fault and error detection, diagnosis and recovery. We will use the term “anomaly” to refer to faults and errors in technical systems. We are particularly interested in examining how Artificial Immune Systems are used to detect deviations and classify them as anomalies based on data acquisition and analysis of symptoms and residuals. We are not interested in disturbances as unknown and/or uncontrolled inputs.

2.2. Causes and consequences of faults

In technical systems, a fault can appear due to external or internal causes (Isermann, 2006). External causes include environmental factors like humidity, dust, chemicals, electromagnetic radiation, high temperature, corrosion, and pollution. Internal causes include missing lubrication, high friction, wear, overheating, leaks, and shortcuts. Faults